Attorney's Docket No. 047347/265025 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Wittkotter Confirmation No.: 2717
Appl. No.: 10/635,798
Filed: August 5, 2003
For: SYSTEMS AND METHODS FOR THE COPY-PROTECTED DISTRIBUTION OF ELECTRONIC DOCUMENTS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUBMITTAL OF PRIORITY DOCUMENT

To complete the requirements of 35 U.S.C. § 119, enclosed is a certified copy of German priority Application No. 102 36 061.8, filed August 6, 2002.

Respectfully submitted,

Scott E. Brient

Scott E. Brient
Registration No. 44,561

Customer No. 00826
Alston & Bird LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
Tel Atlanta Office (404) 881-7000
Fax Atlanta Office (404) 881-7777

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to:
Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on February 25, 2004

Teresa Wells

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	102 36 061.8
Anmeldetag:	06. August 2002
Anmelder/Inhaber:	BrainShield Technologies, Inc., New York, N.Y./US
Bezeichnung:	Vorrichtung zum kopiergeschützten Verteilen elektronischer Dokumente
IPC:	H 04 L, G 06 F

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 02. Oktober 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Ebert

A 9161
06/00
EDV-L

Vorrichtung zum kopiergeschützten Verteilen elektronischer Dokumente

Die vorliegende Erfindung betrifft eine Vorrichtung zum kopiergeschützten Verteilen elektronischer Dokumente einer vorbestimmten Dokumentdatenstruktur in einem öffentlich zugänglichen, elektronischen Datennetz, wie dem Internet, nach dem Oberbegriff des Hauptanspruchs.

Eine derartige Vorrichtung ist beispielsweise aus der deutschen Patentanmeldung 199 50 267 bekannt.

Eine derartige, bekannte Vorrichtung beschreibt, wie mit Hilfe von weitgehend frei verfügbaren und nahezu unbeschränkt verteilbaren, verschlüsselten (Volumen-) Daten und zugehörigen, über einen Rekonstruktionsserver kontrolliert verteilten Rekonstruktionsdateien eine Verteilinfrastruktur für elektronische Dokumente über das Internet, etwa von Text-, Video-, Multimedia- oder Musikdateien, geschaffen werden kann, womit einerseits das berechtigte Interesse der Urheber der oftmals wertvollen (und damit gegen unberechtigtes Kopieren schützenswerten) Dokumente gewahrt ist, und andererseits eine hinsichtlich der übertragbaren Volumina und Serverbelastung tragbare technische Lösung existiert. Allerdings wird gerade die Konzentration auf Server als zentrale Verteilmedien bei dem gattungsbildendem Stand der Technik im Hinblick auf zukünftigen, datenmäßig wesentlich umfangreicheren Content (wie etwa Videodateien, wo bereits ein einziger Videofilm mehrere Gigabyte Volumen aufweist), nicht unproblematisch. Hinzu kommt, dass aufgrund der intensiven öffentlichen Diskussion zur Frage des Urheberrechtsschutzes von digitalem Inhalt (Content) bei Distribution über das Internet gerade serverbasierte Dienste von Nutzern mit Missbrauchsabsicht, sog. Piraten, zunehmend gemieden werden.

Gerade im Zusammenhang mit elektronischen Musikdateien und deren (legalem oder illegalem) Austausch wurde zudem das sog. Napster-Prinzip populär: Eine zentrale Servereinheit erhielt von angeschlossenen Teilnehmerstationen (Clients) Informationen über jeweils bei einem betreffenden Client lokal vorhandenen und elektronisch abrufbaren elektronischen Dateien (typischerweise Musikdateien, die nach dem MP3-Dateiformat codiert sind). Diese aggregierten Verzeichnisdaten der angeschlossenen (verbundenen) Teilnehmer wurden dann wiederum den Teilnehmern zur Suche angeboten, und, etwa bei dem Auffinden des von ihm gewünschten Musikstücks, konnte dann durch entsprechende Übermittlung von Verbindungsdaten der interessierte Teilnehmer unmittelbar mit dem Inhaber der gewünschten Datei einen Datenkontakt aufbauen und im Rahmen dieses Datenkontaktes dann die Datei direkt und unmittelbar laden. Napster funktioniert dabei auf dem Austauschprinzip, wonach von jedem Teilnehmer, dem die Auswahl zur Verfügung steht, erwartet wird, dass er seine Dateien dann wiederum den anderen angeschlossenen Teilnehmern zur Verfügung stellt.

Abgesehen von den potentiellen Urheberrechtsproblemen eines solchen, bekannten Distributionsverfahrens (so wurde insbesondere aus den USA die Napster-Technologie stark kritisiert und hat zu rechtlichen Konsequenzen für die Betreiber geführt), ist jedoch auch hier der generelle Weg über den (die) zentralen Napster-Server potentiell nachteilig: Zunächst würde etwa ein Ausfall des Servers das ganze Netz lahmlegen, zudem führen selbst kleinere Übertragungsprobleme beim unmittelbaren Dateiaustausch zwischen den Clients dazu, dass ein jeweiliger Austausch vollständig wiederholt werden muss, da nach dem Napster-Prinzip serverseitig nur vollständige Dateien namensmäßig identifiziert werden. Zudem ist das System anfällig für Angriffe mit falsch deklarierten oder gar in Schädigungsabsicht manipulierten Inhalten, da zu keinem Zeitpunkt eine Überprüfung auf einen konkreten, etwa dem deklarierten Titel entsprechenden Inhalt erfolgt. Dagegen hat sich das Napster-Prinzip bei der Dist-

ribution elektronischer Dateien (etwa im Hinblick auf das gezielte und effiziente Auffinden spezieller Titel auf einer Vielzahl von angeschlossenen Teilnehmern) als außerordentlich effizient erwiesen.

Nicht zuletzt aufgrund der rechtlichen Probleme beim Betreiben eines derartigen Systems haben sich im folgenden dann zahlreiche alternative Distributionssysteme für elektronischen Content entwickelt. Als Beispiel sei „Gnutella" genannt, wie auch Napster ein sog. Peer-to-Peer-System (da jeweilige Teilnehmer den elektronischen Content unmittelbar zwischen sich austauschen), im Gegensatz zu der serverzentralisierten Steuerung beim Auffinden gewünschter elektronischer Dokumente handelt es sich bei Gnutella jedoch um ein dezentralisiertes Peer-To-Peer-System, d. h. die Anfragen eines ersten Teilnehmers (Suchenden) etwa nach einem Musikstück wird nicht über einen zentralen Titelkatalog in einem Server geleitet (welcher dann, wie bei Napster, eine Zieladresse eines angeschlossenen Peers anbietet), sondern, in der Art einer mehrstufigen und aufgefächerten Kaskade, werden im Gnutella-System mehrstufig eine Vielzahl von Peers unmittelbar abgefragt, und die Abfrage wird bei positivem Auffinden der gewünschten Datei bei einem Peer dann abgebrochen, und es findet die unmittelbare Kontaktaufnahme zwischen den betreffenden Teilnehmern statt.

Im Gegensatz zum zentralisierten System ist das Gnutella-System insbesondere für Fehler weitaus weniger anfällig (kein sog. Single-Point of Failure), dagegen sorgt jedoch kaskadierende Suche für vergleichsweise ineffiziente und damit das Datenvolumen und die jeweiligen Rechenleistungen erhöhende Belastung. Wie auch Napster ist das Gnutella-Verteilverfahren für elektronische Dokumente anfällig gegen elektronische Dateien, die unter dem Titel eines elektronischen Dokuments (z. B. eines Musikstücks) in Schädigungsabsicht missbräuchlich an Dritte versandt werden (oder einfach dem System zum Abruf zur Verfügung stehen); eine Überprüfung auf vertrauenswürdigen Inhalt findet nicht statt

(bzw., etwa wenn die betreffende Datei die Formatkonventionen des entsprechenden Dateityps einhält, wird das Weitergeben letztendlich unbrauchbaren, im schlimmsten Fall sogar schädlichen Inhalts, ungehindert ermöglicht).

Auf weitere Systeme zum kopiergeschützten Verteilen elektronischer Dokumente, etwa Freenet, soll an dieser Stelle nicht näher eingegangen werden. All ihnen ist der Gedanke eines Peer-to-Peer-Netzes in einem öffentlich zugänglichen elektronischen Datennetz gemeinsam, wobei mehr oder weniger effizient bei mehr oder weniger Zugriffskontrolle (insbesondere für einen Urheberrechtsinhaber eines betreffenden elektronischen Dokuments) der elektronische Austausch zwischen angeschlossenen Teilnehmereinheiten erfolgen kann. Während einerseits, wie eingangs diskutiert, der mögliche Flaschenhals einer Datenleitung zu einem reinen serverbasierten System, bei dem über den Server der Inhalt selbst auch zur Verfügung gestellt wird, vermieden werden kann und damit die Ausnutzung des gesamten Netzes wesentlich effizienter wird, so bieten die gerade die Peer-to-Peer-Lösungen, wie diskutiert, neben Grundfragen der Motivation eines Teilnehmers, Dateien zum Download für andere Teilnehmer zur Verfügung zu stellen, das generelle Problem aus der Sicht eines berechtigten Inhabers wertvollen elektronischen Inhalts, wie die Verteilung dieses elektronischen Inhalts (bzw. der zugehörigen elektronischen Dateien) wirksamer gesteuert bzw. kontrolliert werden kann. Neben der Problematik der Urheberrechtsverletzungen steht daher die grundsätzliche Problematik eines Anreizsystems von Urhebern elektronischer Inhalts, überhaupt weiterer elektronischer Werke zu schaffen, wenn diese, etwa mittels faktisch unkontrollierbarer Peer-to-Peer-Systeme, frei und allgemein verteilt werden.

Aufgabe der vorliegenden Erfindung ist es daher, auch für das Umfeld von Peer-to-Peer-Systemen in öffentlich zugänglichen elektronischen Datennetzen, insbesondere dem Internet, eine verbesserte Infrastruktur zur elektronischen Dis-

Distribution wertvoller (und potentiell schützenswerter) elektronischer Dokumente zu schaffen, womit einerseits effizient und zuverlässig die Distribution des Contents (d. h. der Dokumente) stattfinden kann, und andererseits die Rechte des Urhebers an dem betreffenden elektronischen Dokuments, mithin also an der Verteilung bzw. Distribution desselben, besser kontrolliert und geschützt werden können.

Die Aufgabe wird durch die Vorrichtung mit den Merkmalen des Hauptanspruchs sowie der unabhängigen Patentansprüche 5 und 13 gelöst; vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen beschrieben.

In Weiterentwicklung der Grundgedanken der DE 199 50 267 findet auch bei der Vorrichtung nach der vorliegenden Erfindung eines Distribution elektronischer Dokumente über das elektronische Datennetz statt, und zwar in der Art eines Peer-to-Peer-Netzes zwischen Teilnehmern des mit der Erfindung geschaffenen Übertragungs- und Austauschsystems. Als „Teilnehmer" (bzw. „Teilnehmereinheit") im Rahmen der Erfindung soll dabei diejenige, einem jeweiligen, identifizierten Benutzer zugeordnete Einheit verstanden werden, die typischerweise als PC-Arbeitsplatz oder andere, mit dem Internet verbundene Einheit eingerichtet ist, unabhängig (und normalerweise auch unbekannt) von/gegenüber einem anderen Teilnehmer ist und gängige Speicher- und Ladezugriffe (Upload/Download) über das Internet durchführen kann.

Im Rahmen der Erfindung und zur Realisierung eines Peer-to-Peer-Netzes ist dabei zunächst vorgesehen, dass jedes elektronische Dokument, etwa eine Musikdatei oder ein elektronischer Video-Film, in eine Mehrzahl von Dateiabschnitten untergliedert ist. Typischerweise handelt es sich dabei, etwa im Fall einer MP3-Musikdatei, um die jeweiligen MP3-Frames nach dem Dokumentformatstandard. Charakteristisch für die Erfindung ist zunächst, dass die einem jeweiligen elektronischen Dokument zugeordnete Mehrzahl von Dateiabschnitten auf mindestens einer anderen (bezogen auf den Su-

chenden) Teilnehmereinheit abgelegt ist, wobei auf keiner Teilnehmereinheit das elektronische Dokument als Anordnung der zugehörigen Dateiabschnitte so vorliegt, dass das elektronische Dokument in seiner ursprünglichen Form für den Benutzer brauchbar ist. Mit anderen Worten, es liegt lediglich in verschlüsselter Form, nämlich geschaffen durch die (gegenüber der Ursprungsform abweichende) Anordnung der Dateiabschnitte vor.

Damit nun ein angeschlossener Teilnehmer (der Suchende) auf ein von ihm gewünschtes elektronischer Dokument zugreifen kann, erhält dieser von der erfindungsgemäßen Befehlsdateneinheit eine Sequenz von elektronischen Ablaufsbefehlsdaten, die, neben einer vorbestimmten (typischerweise dem Suchenden individuell zugeordneten) Reihenfolge der Dateiabschnitte, auch Angaben über einen jeweiligen Speicherort (Adresse) der jeweiligen Dateiabschnitte aufweist (typischerweise bei mindestens einem, in der Regel bei mehreren anderen, angeschlossenen Teilnehmereinheiten). Durch das Ablaufen der elektronischen Ablaufbefehlsdaten bei dem Teilnehmer (Suchenden) im Rahmen dessen Internetzugriffsinfrastruktur (typischerweise wird die beschriebene Funktionalität mit Hilfe eines Plug-Ins in einen herkömmlichen Browser realisiert) entsteht dann bei dem Suchenden wiederum eine Mehrzahl geladener elektronischer Dateiabschnitte, die dem gewünschten elektronischen Dokument zugehörig sind (allerdings liegen diese üblicherweise teilnehmerseitig wiederum auch verschlüsselt, d. h. nicht in der ursprünglichen und damit nicht in der brauchbaren Abfolge vor).

Um nun teilnehmerseitig das elektronische Dokument so wiederzugeben, wie es der ursprünglichen, unverschlüsselten und zur Benutzung geeigneten bzw. vorgesehenen Form entspricht, bedarf es erfindungsgemäß eines Kontakts mit der Rekonstruktionseinheit, die, typischerweise als Servereinheit mit dem elektronischen Datennetz (Internet) verbunden, auf entsprechende teilnehmerseitige Anforderung (und typischerweise nach geeigneter Autorisierung, Validierung bzw.

dem Durchführen eines kommerziellen Transaktionsvorganges) dem jeweiligen Teilnehmer die erfindungsgemäß Rekonstruktionsdatei zur Verfügung stellt, womit dieser dann die gewünschte, brauchbare Form des elektronischen Dokuments teilnehmerseitig herstellen kann. Dabei besteht im einfachsten Fall die Rekonstruktionsdatei aus Index- bzw. Sequenzangaben, welche die Mehrzahl der Dateiabschnitte (die teilnehmerseitig noch nicht in der brauchbaren Form und damit (individuell) verschlüsselt vorliegen) in die brauchbare Form gebracht und damit entschlüsselt werden können.

Zusätzlich ist der empfangende Teilnehmer (Suchende) für Zugriffe durch Dritte auf die geladenen Dateiabschnitte selbst wiederum Partner und potentielle Quelle für das Laden.

Im Ergebnis kann durch dieses erfindungsgemäße Vorgehen einerseits der Effizienzvorteil von Peer-to-Peer-Netzwerken gegenüber serverbasierten Distributions-Netzwerken sinnvoll eingesetzt werden, andererseits ermöglicht es das erfindungsgemäße Zusammenwirken von über die Befehlsdateneinheit bereitgestellter Ablaufbefehlsdaten sowie der serverbasierten Rekonstruktionseinheit, ein effizientes, gleichzeitig den Urheberrechtsschutz von Berechtigten an elektronischem Inhalt schützendes System zu realisieren, mithin also ein Maß an Kontrolle zu behalten, welches für das Vermeiden missbräuchlicher Distribution elektronischer Dokumente notwendig ist.

Dabei ist es üblich und bevorzugt, dass das elektronische Dokument in der (für den Teilnehmer) brauchbaren Form zu keinem Zeitpunkt bei einer der Teilnehmereinheiten in der korrekten Abfolge (d. h. unverschlüsselt und brauchbar) vorliegt; vielmehr ist das betreffende elektronische Dokument stets in der beschriebenen Weise verschlüsselt, wobei sich weiterbildungsgemäß insbesondere die auch als „semantische Verschlüsselung" bekannten Operationen des Vertauschens, Entfernens, Hinzufügens und/oder Austauschens von

Dateiabschnitten zum Herstellen der verschlüsselten Form als besonders bevorzugt herausgestellt haben. Insoweit wird Bezug genommen auf die zugrundeliegende DE 199 50 267, welche insbesondere hinsichtlich der Erzeugung einer entsprechenden verschlüsselten elektronischen Datei als elektronisches Dokument in die vorliegende Anmeldung als zur Erfindung gehörig einbezogen gelten soll; entsprechendes gilt für die in der Internationalen Patentanmeldung PCT/EP00/06824 (WO01/06341) beschriebene Vorrichtung zum Erzeugen der jeweiligen elektronischen Dateiabschnitte als semantische Elemente aus der Dokumentdatenstruktur des ursprünglichen elektronischen Dokuments.

Weiterhin ist es besonders bevorzugt, das vorliegende erfindungsgemäße Distributionssystem insbesondere auch zum Vertrieb elektronischer Dokumente zu benutzen, d. h. dem betreffenden Teilnehmer als Benutzer die Wiederherstellung des von ihm in der beschriebenen Weise im Peer-to-Peer-Netz geladenen Dokuments in die unverschlüsselte, brauchbare Form durch Zugriff auf die Rekonstruktionseinheit erst nach dem Durchführen eines entsprechenden Transaktionszuganges (z. B. durch die Eingabe von Zahlungsdaten, wie etwa Kreditkartennummer od. dgl.) zu ermöglichen.

Umfasst von der vorliegenden Erfindung ist es auch, jeder erfindungsgemäßen Teilnehmereinheit im Sinne der Erfindung die Publikation eigner elektronischer Dokumente über das erfindungsgemäße System zu ermöglichen. Hierzu ist zunächst das Aufteilen des entsprechenden (unverschlüsselten) elektronischen Dokuments in die Mehrzahl von Dateiabschnitten notwendig; der entsprechende Schritt, auch als „semantische Analyse bzw. Verschlüsselung" bezeichnet, besteht zunächst in dem Identifizieren der typischerweise durch das jeweilige Dokumentformat gegebenen Dokumentformatstruktur und dem Aufteilen in unabhängig voneinander nutzbare, inhaltswirksame Komponenten als Dateiabschnitte (etwa Frames bei MP3 oder Videodateien; Sätze, Wörter oder Absätze bei Textdateien; Bildelemente bei Bilddateien usw.).

Daraufhin wird dann eine den Verschlüsselungseffekt bewirkende, der ursprünglichen Form (z.B. Reihenfolge) üblicherweise nicht mehr entsprechende Anordnung der Dateiabschnitte geschaffen, wobei diese Anordnung dann die für das Laden im Peer-to-Peer-System notwendigen Ablaufbefehlsdaten vorgibt bzw. bestimmt (und eine Rekonstruktion in die ursprüngliche, unverschlüsselte Abfolge dann mittels der von der Rekonstruktionseinheit heranzuführenden Rekonstruktionsdatei erfolgt). Zur Realisierung der Publikationsfunktion ist dann die Teilnehmereinheit eingerichtet, die jeweiligen elektronischen Dateiabschnitte auf einer oder mehreren anderen Teilnehmereinheiten abzulegen sowie dokumentidentifizierende Daten, typischerweise einen zugehörigen Titel des elektronischen Dokuments, einer üblicherweise zentralen Dokumentnamenseinheit zur Verfügung zu stellen.

Auf diese Weise wird die vorliegende Erfindung sowohl publikations- als auch leserseitig zu einem vollwertigen Distributionssystem, welches lediglich zur Entschlüsselung über die Rekonstruktionseinheit Serverunterstützung benötigt (und wobei die elektronischen Ablaufbefehlsdaten entweder auch von einer geeigneten Servereinheit herbeigeführt werden können, oder aber in dem beschriebenen Peer-to-Peer-System, als Funktionalität der Teilnehmereinheiten selbst, bereitgestellt werden können).

Weitere Vorteile, Merkmale und Einzelheiten der Erfindung ergeben sich aus der nachfolgenden Beschreibung bevorzugter Ausführungsbeispiele sowie anhand der Figuren; diese zeigen in

Fig. 1: ein schematisches Blockschaltbild der Vorrichtung zum kopiergeschützten Verteilen elektronischer Dokumente gemäß einer ersten Ausführungsform der vorliegenden Erfindung und

Fig. 2: ein analoges, schematisches Blockschaltbild zum Verdeutlichen einer Weiterbildung der vorliegenden Erfindung mittels Proxyeinheit.

Mit schematischen Funktionsblöcken ist in der Fig. 1 eine erste Ausführungsform der vorliegenden Erfindung als Internet-basiertes System zum kopiergeschützten Verteilen elektronischer Dokumente skizziert; es soll für die weitere Beschreibung das Ausführungsbeispiel angenommen werden, dass mittels der in Fig. 1 gezeigten Ausführungsform elektronische Musikdateien des MP3-Formats über das Internet verteilt werden sollen.

Es handelt sich bei dem Ausführungsbeispiel um ein Peer-to-Peer-System mit einer Mehrzahl von Teilnehmereinheiten 10, jeweils begrenzt durch die einfach gestrichelten Linien.

Genauer gesagt weist jede Teilnehmereinheit, die typischerweise auf einem clientseitigen PC mit gängiger Internet-Zugangsinfrastruktur realisiert ist, wobei die gezeigten Funktionalitäten durch Plug-Ins für einen jeweils verwendeten Browser realisiert sind, mindestens vier miteinander zusammenwirkende Funktionseinheiten auf: Zunächst ist eine Content-Speichereinheit 12 zum lokalen (d. h. teilnehmerseitigen) Ablegen der MP3-Dateien als elektronischer Dokumente in Form einer Anordnung einzelner Dateiabschnitte ei-

nes jeweiligen Dokuments, genauer gesagt von Einzelframes bzw. Frameblöcken der MP3-Datei, vorgesehen, und zwar erfolgt das Ablegen in verschlüsselter Form so, dass die Abfolge der MP3-Dateiabschnitte nicht der ursprünglichen, brauchbaren Form entspricht. Mit anderen Worten, würde man die MP3-Dateiabschnitte in der abgelegten (verschlüsselten) Form wiedergeben, z. B. durch eine (nicht gezeigte, aber ansonsten bekannte) Wiedergabeeinheit der Teilnehmereinheit 10, würde sich ein unzusammenhängender und damit nicht brauchbarer Klangeffekt bei der Musikwiedergabe ergeben.

Neben der Content-Speichereinheit 12 weist jede Teilnehmereinheit 10 eine Publikationseinheit 14 auf. Diese hat die Aufgabe, dem betreffenden Teilnehmer die Publikation eigener kopiergeschützter Inhalte (hier: MP3-Musikdateien) über das erfindungsgemäße System zu ermöglichen. Genauer gesagt ist die Publikationseinheit 14 zunächst ausgebildet, eine zu publizierende MP3-Musikdatei in Dateiabschnitte zu zerlegen und aus diesen eine Anordnung zu bilden, die nicht der brauchbaren Form (d. h. bei der Wiedergabe zum Original-Musikstück führenden Form) entspricht. Zu diesem Zweck weist die Publikationseinheit in der in Fig. 1 nicht näher gezeigten Weise Einheiten zur Strukturanalyse der zu publizierenden MP3-Datei auf, sowie ferner Einheiten, welche die den Verschlüsselungseffekt bewirkende Anordnung, etwa durch Operationen des Vertauschens, Einfügens usw. von einzelnen Dateiabschnitten (MP3-Frames oder Blöcke von diesen) vornimmt. Weiterhin ist in die Publikationseinheit vorgesehen, vgl. den gezeigten Pfeil zur Content-Speichereinheit 12' einer weiteren, mit dem Internet verbundenen Teilnehmereinheit 10', die so erzeugten Dateiabschnitte bei anderen Teilnehmereinheiten (bzw. deren Content-Speichereinheiten) abzulegen; möglich ist auch, dass ein Teil der erzeugten Dateiabschnitte auf der eigenen Content-Speichereinheit 12 abgelegt werden.

Um im Rahmen des erfindungsgemäßen Peer-to-Peer-Systems den Zugriff durch andere Teilnehmereinheiten zu ermöglichen,

stellt die Publikationseinheit 14 gleichzeitig identifizierende Daten für die publizierte Musikdatei, nämlich den Titel sowie die Adresse bzw. den Ablageort (Abspeicherungsort) der betreffenden Dateiabschnitte, einer Dokumentnamenseinheit 20 (Titel) bzw. einem Volumendatenverzeichnis 22 (Adressen bzw. Abspeicherungsorte) zur Verfügung; beide Einheiten 20, 22 werden typischerweise als Netz-Services angeboten und auf geeigneten Servereinheiten im Internet vorgesehen (möglich ist aber auch, dass die Einheiten 20 bzw. 22 wiederum als Funktionalitäten jeder Teilnehmereinheit 10 vorgesehen sind).

Schließlich stellt die Publikationseinheit 14 die Publikationsdaten, insbesondere die Information über eine Rekonstruktion des verschlüsselt abgelegten Dokuments (hier: die korrekte, ein ordnungsgemäßes Abspielen des MP3-Dokuments ermöglichende Reihenfolge der Dateiabschnitte) sowie weitere, distributionsrelevante Daten, insbesondere mögliche Benutzungsrechte von Dritten sowie weitere Konditionen für einen Zugriff durch Dritte, einer serverbasierten Rekonstruktionseinheit 30 zur Verfügung, deren Aufbau und Funktionalität unten im Zusammenhang mit dem Zugriffs- und Wiedergabevorgang beschrieben wird. Mit diesen Vorgängen wäre zunächst der Publikationsvorgang, durchgeführt durch die Publikationseinheit 14, abgeschlossen.

Als nächste Funktionseinheit der Teilnehmereinheit 10 ist die Zugriffseinheit 16 teilnehmerseitig vorgesehen, dem betreffenden Teilnehmer seinerseits Zugriff im Wege des Peer-to-Peer-Netzes auf verteilt bei anderen Teilnehmereinheiten vorliegende Detailabschnitte von elektronischen Dokumenten zu ermöglichen.

Zu diesem Zweck ist die Zugriffseinheit 16 zunächst eingerichtet, auf die Dokumentnamenseinheit 20 zuzugreifen. Der Benutzer hat hier die Möglichkeit, das von ihm gewünschte Musikstück namensmäßig zu identifizieren und entsprechend über eine üblicherweise serverbasiert vorgesehene Script-

einheit 24 eine entsprechende Abfolge von Befehlsdaten abzufordern, welche dann, entsprechend der durch die Befehlsdaten (Script) vorgegebenen Abfolge sowie der im Volumendatenverzeichnis 22 gespeicherten, jeweiligen Adressen das scriptgesteuerte Zugreifen auf jeweilige Content-Speichereinheiten 12, 12' von verschiedenen Teilnehmereinheiten des elektronischen Datennetzes ermöglicht. Als Ergebnis dieses Zugriffs liegt dann lokal in der Teilnehmereinheit 10 eine Mehrzahl von Dateiabschnitten des gewünschten Musikstücks vor, und zwar in der nicht für die Wiedergabe brauchbaren (d. h. verschlüsselten) Abfolge.

Zusätzlich ist es im Rahmen des in Fig. 1 skizzierten Ausführungsbeispiels vorgesehen, diesem Zugriffsvorgang eine Überprüfung mittels einer serverbasierten Signaturservereinheit 40 vorzuschalten, welche, insbesondere mittels für ein betreffendes Musikstück charakteristischen Signatur, die Überprüfung ermöglicht, ob es sich überhaupt bei dem zu ladenden bzw. gewünschten Musikstück um eine dem tatsächlichen Musikstück entsprechende MP3-Datei handelt, welche dann für das erfindungsgemäße Verteilen geeignet und vorgesehen ist; wie in der Fig. 1 gezeigt, besteht von der Signatur-Servereinheit 40 zusätzlich eine Beziehung zur Rekonstruktionseinheit 30. Eine weitere oder alternative Funktionalität der Einheit 40 (oder einer zusätzlichen Einheit) besteht darin, auf der Basis einer etwa verlags- oder urheberseitig vorliegenden Dokumentsignatur zu überprüfen, ob ein entsprechendes, zur Publikation vorgesehenes Dokument überhaut die verlags- oder urheberseitige Distributionsberechtigung besitzt (insoweit besteht auch eine Verbindung zur Publikationseinheit 14).

Als vierte Funktionalität jeder Teilnehmereinheit 10 ist eine Entschlüsselungseinheit 18 vorgesehen. Diese dient dazu, die Mehrzahl von mittels der Zugriffseinheit 16 verteilt aus dem Netz geladenen Dateiabschnitte der gewünschten MP3-Musikdatei zu entschlüsseln bzw. zu rekonstruieren und damit in die brauchbare Form zu bringen. Erfindungsge-

mäß ist dies nur durch einen Kontakt mit der Rekonstruktionseinheit 30 möglich, wobei die Entschlüsselungseinheit 18 der Teilnehmereinheit 10 diesen Rekonstruktions- bzw. Entschlüsselungsvorgang initiiert. Genauer gesagt weist die Rekonstruktionseinheit 30 eine Freigabe-Servereinheit 32 auf, welche zum einen, mittels einer nachgeschalteten Benutzerrechteeinheit 34 sowie einer verbundenen eShop-Servereinheit 36, überprüft, ob der betreffende, mittels seiner Entschlüsselungseinheit 18 zugreifende Teilnehmer überhaupt eine Zugriffs- (und damit Entschlüsselungs-) Berechtigung besitzt (Einheit 34), bzw. eine in einem Transaktionsdialog durchzuführende Zahlung (Einheit 36) geleistet hat; typischerweise gibt es die Möglichkeit, das Recht zum Wiedergeben eines unverschlüsselten Musikstücks teilnehmerseitig von der Rekonstruktionseinheit 30 (bzw. der eShop-Servereinheit 36) gegen Bezahlung od. dgl. Vergütungsinstrument zu erwerben. Eine Entschlüsselungseinheit 38 ermöglicht dann der Freigabeeinheit 32 das Übermitteln einer Rekonstruktionsdatei zum Herstellen einer unverschlüsselten, für die Wiedergabe brauchbaren Form des elektronischen Dokuments (d. h. der MP3-Musikdatei), indem im beschriebenen Ausführungsbeispiel die Rekonstruktionsdatei von der Entschlüsselungseinheit 16 benutzt wird, um die teilnehmerseitig vorliegenden Dateiabschnitte in die für eine brauchbare Wiedergabe geeignete Reihenfolge zu bringen. Um nachgelagerten Missbrauch nach dem lokalen (teilnehmerseitigen) Wiederherstellen des elektronischen Dokuments zu verhindern, ist bei dem beschriebenen Ausführungsbeispiel vorgesehen, dass der Teilnehmer keine Möglichkeit hat, die in der korrekten Anordnung wiederhergestellte, brauchbare Musikdatei in der brauchbaren Form abzuspeichern.

Die vorliegende Erfindung ist nicht auf das in Fig. 1 beschriebene Ausführungsbeispiel beschränkt; beliebige Varianten sind denkbar, etwa die kritischen Funktionskomponenten des Volumendatenverzeichnisses, der Dokumentnamensein-

heit oder der Scriptservereinheit serverbasiert oder wiederum netzverteilt vorzusehen.

Die Fig. 2 verdeutlicht zudem eine Weiterbildung, bei welcher der Teilnehmereinheit 10 eine Proxyeinheit 50 zugeordnet und vorgeschaltet ist. Wie aus der Fig. 2 erkennbar ist, übernimmt, bei ansonsten gleicher Funktionalität, die Proxyeinheit 50 für die Teilnehmereinheit 10, dort insbesondere die Publikationseinheit 14 und die Zugriffseinheit 16, publikationsseitig den Kontakt mit dem Volumendatenverzeichnis 22, der Dokumentnamenseinheit 20 sowie einer Content-Speichereinheit 12' eines weiteren Netzteilnehmers. Downloadseitig würde die Proxyeinheit 50 dann für die Zugriffseinheit 16 einer Teilnehmereinheit 10 den Kontakt mit der Scriptservereinheit 24 herstellen sowie, Script- (Befehlsdaten-) gesteuert durch diese, dann den Ladezugriff auf jeweilige, bei Peers im Netz verteilte Content-Speichereinheiten 12' vornehmen.

Eine derartige Konfiguration hätte den Vorteil, die Teilnehmereinheit zu entlasten, gleichzeitig damit eine unabhängige Einheit für den Zugriff im Peer-to-Peer-Netz zur Verfügung zu stellen.

Im Ergebnis werden durch die vorliegende Erfindung zahlreiche Vorteile realisiert. Insbesondere ist es durch die serverbasierte Rekonstruktionseinheit (bzw. der in Fig. 1, Fig. 2 gezeigten Freigabe-Servereinheit) jederzeit problemlos möglich, eine weitere Publikation, ggf. sogar eine aktuelle Nutzung eines elektronischen Dokuments jederzeit und zentral zu unterbinden (insbesondere wenn, wie weiterbildungsgemäß vorgesehen, jeder Dokumentzugriff einen zumindest einmaligen (temporären) Zugriff auf die Rekonstruktionseinheit 30 notwendig macht).

Sollte sich herausstellen, dass etwa über das Netz inhaltlich manipulierte bzw. gefälschte elektronische Dokumente publiziert werden, kann insbesondere jegliche Nutzung die-

ses Inhaltes nach der ersten Erkennung sofort unterbunden werden (es würde eine entsprechende, üblicherweise automatisierte Meldung an die Skriptserver- bzw. -erzeugungseinheit geleitet werden, wodurch dann zukünftige Zugriffsprozesse auf das Dokument ausgeschlossen werden).

Gleichzeitig bleiben sämtliche Vorteile eines Peer-to-Peer-Netzes im Hinblick auf Effizienz der Datenübertragung und Gleichmäßigkeit der Belastung der Datenleitungen erhalten; insbesondere steht jedes von einer Teilnehmereinheit für den lokalen Gebrauch geladene Dokument ja selbst auch wieder mit seinen Datenabschnitten für eine weitere Distribution resp. den Zugriff durch Dritte zur Verfügung.
Ein weiterer Vorteil des Systems liegt darin, dass, bewirkt durch die Publikationseinheit 14, jeder Teilnehmer selbst auch publizieren kann.

Der Inhalt (d. h. die jeweiligen elektronischen Dokumente) liegen in den jeweiligen Content-Speichereinheiten 12 jeder Teilnehmereinheit verschlüsselt vor und sind damit jederzeit urheberrechtlich, insbesondere auch im Hinblick auf unberechtigte Weitergabe, geschützt.

Im Hinblick auf Kommunikationsfehler im Netz bzw. das Zusammenbrechen einzelner Knoten weist die beschriebene Vorrichtung die Vorteile eines Peer-to-Peer-Netzes auf, d. h. es kann üblicherweise ein entsprechender, benötigter Dateiabschnitt auch von einem anderen Peer geladen werden, wenn etwa bei einem Download eine Verbindung zu einer Teilnehmereinheit zusammenbricht.

Ein weiterer Vorteil im Hinblick auf das Unterbinden von Urheberrechtsverletzungen und Missbrauch liegt darin, dass weiterbildungsgemäß von einem elektronischen Dokument, etwa einem Musikstück, durch jeweilige individuelle Anordnung der Dateiabschnitte benutzerindividuelle (und damit identifizierende) Verschlüsselungsvarianten existieren. Werden diese nunmehr unoutorisiert weitergegeben, lässt sich damit

die Quelle für einen Missbrauch problemlos erkennen, nämlich durch Abgleich einer entsprechenden Version mit dem zugehörigen, einem Teilnehmer zur Verfügung gestellten Script (d. h. den individuellen Ablaufbefehlsdaten).

Über die oben beschriebenen Versionen und deren Vorteile und Funktionalität hinaus sind zahlreiche Weiterentwicklungen und spezielle Konfigurationen denkbar:

So ist es insbesondere sinnvoll, ein Kompensations- bzw. Belohnungssystem dafür zu schaffen, dass ein jeweiliger Teilnehmer (Peer) als Teilnehmer des Distributionsnetzes aktiv und Online bleibt und insoweit selbst auch für Downloads von Dritten zur Verfügung steht (auch wenn, durch die inhärente Unsymmetrie zwischen Upload- und Downloadkanal der meisten Hochgeschwindigkeit-Internet-Zugänge von Teilnehmern bereits eine gewisse Motivation zur Teilnahme darin liegt, dass das Herunterladen durch einen Teilnehmer (und die damit erreichbare Geschwindigkeit) durch den typischerweise langsameren Upload-Kanal des betreffenden Partners begrenzt ist und insoweit das simultane Laden von mehreren Teilnehmern wünschenswert ist.

Weiterbildungsgemäß wäre es nützlich, etwa die Dokumentnamenseinheit der Fig. 1 mehrfach in Form eines Directories vorzusehen, etwa mit überlappenden Angeboten. Es ergibt sich hier die Möglichkeit zur Spezialisierung auf Themen, etwa durch entsprechende zugeordnete Metadaten. Auch ist es möglich, wie bereits vorstehend diskutiert, derartige Content-Verzeichnisse dezentral vorzusehen. Insbesondere könnte dann eine Inhaltssuche kaskadiert erfolgen, wie eingangs anhand des Gnutella-Vorgangs diskutiert.

Entsprechend ist es möglich, die Scriptservereinheit 24 mehrfach vorzusehen; im Hinblick auf den Ausfall einer solchen Einheit wird damit die Zuverlässigkeit des Netzes deutlich erhöht. Letztendlich eignet sich diese zentrale bzw. verteilte Scripterzeugung auch dafür, gewisse Inhalte

für gewisse Territorien (bzw. gewisse Internet-Angebote) dezidiert anzubieten.

Eine besonders bevorzugte Weiterbildung ist es, Informationen über die Unterteilung des Dokuments in Dateiabschnitte bzw. Hinweise auf eine mögliche Rekonstruktionsdatei in dem Dokument selbst vorzusehen, etwa innerhalb des sog. ID3-Records (also als Teil der Dokument-Struktur) bei MP3; auch wäre es möglich, hier etwa die Adresse des zugehörigen Rekonstruktionsservers abzulegen.

PATENTANSPRÜCHE

1. Vorrichtung zum kopiergeschützten Verteilen elektronischer Dokumente einer vorbestimmten Dokumentdatenstruktur in einem öffentlich zugänglichen, elektronischen Datennetz, insbesondere dem Internet, mit
   - einer Mehrzahl von mit dem elektronischen Datennetz zumindest zeitweise verbundenen, jeweils einem Benutzer zugeordneten Teilnehmereinheiten, die zum Durchführen eines Ladezugriffs auf ein elektronisches Dokument von einer mit dem Datennetz verbundenen Teilnehmer- oder Servereinheit sowie zum Öffnen des elektronischen Dokuments mittels einer benutzerseitig vorgesehenen Wiedergabeeinheit ausgebildet sind,

   dadurch gekennzeichnet, dass
   - die Teilnehmereinheiten zum jeweiligen Zugreifen auf das elektronische Dokument über das öffentlich zugängliche elektronische Datennetz so ausgebildet sind, dass eine Mehrzahl von Ladezugriffen auf eine Mehrzahl zugehöriger elektronischer Dateiabschnitte durchgeführt wird, wovon mindestens ein Ladezugriff von einer jeweils anderen, einem anderen Benutzer zugeordneten Teilnehmereinheit erfolgt,
   - zum Durchführen der Mehrzahl von Ladezugriffen die Teilnehmereinheiten dokument- und/oder teilnehmerspezifisch erstellte elektronische Ablaufbefehlsdaten von einer mit dem elektronischen Datennetz verbundenen Befehlsdateneinheit, insbesondere einer Befehlsdaten-Servereinheit, erhalten,
   - die Mehrzahl der durch die Ladezugriffe benutzerseitig vorliegenden, dem elektronischen Dokument zugehörigen elektronischen Dateiabschnitte eine durch eine durch Wirkung der Ablaufbefehlsdaten bestimmte Anordnung von Dateiabschnitten ver-

schlüsselte Form des elektronischen Dokuments darstellen, die für den Benutzer nicht in der vorgesehenen Weise brauchbar ist,

- mit dem elektronischen Datennetz eine Rekonstruktionseinheit, insbesondere Rekonstruktions-Servereinheit, verbunden ist, die zum Speichern einer Mehrzahl von einem elektronischen Dokument in der verschlüsselten Form zugeordneten Rekonstruktionsdateien ausgebildet ist,
- und die Teilnehmereinheiten jeweils eine lokale Entschlüsselungseinheit aufweisen, die zum für jedes elektronische Dokument mindestens einmaligen Zugreifen auf die Rekonstruktionseinheit über das elektronische Datennetz und zum Zusammenführen der verschlüsselten Form mit einer Rekonstruktionsdatei zum Erzeugen des elektronischen Dokuments zur Wiedergabe durch die Wiedergabeeinheit in für den Benutzer brauchbarer, unverschlüsselter Form ausgebildet ist.

2. Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, dass die Teilnehmereinheiten so ausgebildet sind, dass das elektronische Dokument in der für den Benutzer brauchbaren, unverschlüsselten Form benutzerseitig nicht abspeicherbar ist.

3. Vorrichtung nach Anspruch 1 oder 2, gekennzeichnet durch eine der Rekonstruktionseinheit zugeordnete Benutzeridentifikations- und/oder Abrechnungseinheit, die zum Erfassen von einen Benutzer individualisierende Daten, zum Durchführen einer finanziellen Transaktion mit dem Benutzer und/oder zum Zuordnen oder Verwalten von Benutzer- oder Benutzergruppen spezifischen Zugriffsrechten ausgebildet ist.

4. Vorrichtung nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass für das Empfangen der Ablaufbefehlsdaten sowie das Durchführen der Mehrzahl von La-

dezugriffen einer betreffenden Teilnehmereinheit eine mit dem elektronischen Datennetz verbundene Proxyeinheit zugeordnet ist.

5. Vorrichtung zum kopiergeschützten Verteilen elektronischer Dokumente einer vorbestimmten Dokumentdatenstruktur in einem öffentlich zugänglichen, elektronischen Datennetz, insbesondere nach einem der Ansprüche 1 bis 4, mit

- einer Mehrzahl von mit dem elektronischen Datennetz zumindest zeitweise verbundenen, jeweils einem Benutzer zugeordneten Teilnehmereinheiten, die zum Durchführen eines Ladezugriffs auf ein elektronisches Dokument von einer mit dem Datennetz verbundenen Teilnehmer- oder Servereinheit sowie zum Öffnen des elektronischen Dokuments mittels einer benutzerseitig vorgesehenen Wiedergabeeinheit ausgebildet sind,

dadurch gekennzeichnet, dass

die Teilnehmereinheiten jeweils eine Publikationseinheit aufweisen, die

zum Aufteilen des elektronischen Dokuments in eine Mehrzahl von Dateiabschnitten,

zum Erzeugen einer durch Anordnung der Dateiabschnitte verschlüsselten Form eines kopiergeschützt zu verteilenden elektronischen Dokuments, wobei die Anordnung durch Ablaufbefehlsdaten bestimmt ist,

zum Übertragen und/oder Ablegen der Mehrzahl elektronischer Dateiabschnitte auf mindestens einer jeweils anderen Teilnehmereinheit sowie

zum Eintragen dokumentidentifizierender, bevorzugt öffentlicher Daten in eine mit dem elektronischen Datennetz verbundene Dokumentnamenseinheit, insbesondere Dokumentnamenservereinheit,

ausgebildet sind,

wobei eine mit dem elektronischen Datennetz verbundene, bevorzugt zentrale Dateiservereinheit Daten über

die bei der mindestens einen anderen Teilnehmereinheit abgelegten elektronischen Dateiabschnitte als Grundlage für ein Erzeugen der Ablaufbefehlsdaten enthält.

6. Vorrichtung nach Anspruch 5, gekennzeichnet durch eine mit der Dateiservereinheit zusammenwirkende Scripterzeugungseinheit, die zum Erzeugen der Ablaufbefehlsdaten ausgebildet ist und als Scriptservereinheit oder als Teil der Teilnehmereinheit ausgebildet ist.

7. Vorrichtung nach Anspruch 5 oder 6, dadurch gekennzeichnet, dass die Publikationseinheit eine Identifikations- und/oder Verifikationseinheit für das kopiergeschützt zu verteilende elektronische Dokument aufweist, welche zum insbesondere signaturbasierten Überprüfen eines kopiergeschützt zu verteilenden elektronischen Dokuments auf benutzerseitige Berechtigung, zum Verhindern des Erzeugens, Aufteilens, Übertragens und/oder Ablegens als Reaktion auf eine Berechtigungsüberprüfung sowie bevorzugt zum Abgleich dokumentspezifischer Identifikationsdaten mit Identifikationsdaten einer mit dem elektronischen Datennetz verbundenen Identifikations-Servereinheit ausgebildet ist.

8. Vorrichtung nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass das Erzeugen der verschlüsselten Form des elektronischen Dokuments mittels einer Verschlüsselungseinheit als Teil der Publikationseinheit und/oder das Erzeugen des elektronischen Dokuments in der unverschlüsselten Form mittels der lokalen Entschlüsselungseinheit die folgenden Operationen auf Dateiabschnitte der Dokumentdatenstruktur des elektronischen Dokuments aufweist: Vertauschen und/oder Entfernen eines Dateiabschnitts und/oder Hinzufügen eines Dateiabschnitts an eine vorbestimmte Position

in einer Folge von Dateiabschnitten und/oder Austauschen eines Dateiabschnitts gegen einen bevorzugt im ursprünglichen elektronischen Dokument nicht enthaltenen Dateiabschnitt, insbesondere mittels eines Rechnerzugriffs auf jeweilige, den Dateiabschnitten der Dokumentdatenstruktur zugeordnete elektronische Speicherbereiche der elektronischen Verschlüsselungseinheit bzw. der lokalen Entschlüsselungseinheit.

9. Vorrichtung nach Anspruch 8, dadurch gekennzeichnet, dass die elektronische Verschlüsselungseinheit zum Erzeugen der Rekonstruktionsdatei mit Angaben über die vertauschten, entfernten, hinzugefügten und/oder ausgetauschten Dateiabschnitte ausgebildet ist.

10. Vorrichtung nach Anspruch 8 oder 9, dadurch gekennzeichnet, dass der Teilnehmereinheit Formaterkennungsmittel zugeordnet sind, die teilnehmerseitig die Feststellung ermöglichen, ob ein elektronisches Dokument durch ein Vertauschen, Entfernen, Hinzufügen und/oder Austauschen von Dateiabschnitten verschlüsselt wurde, und die insbesondere aus mindestens einem Dateiabschnitt eine Adresse zum Zugreifen auf die Rekonstruktionsdaten extrahieren.

11. Vorrichtung nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, dass das elektronische Dokument eine Audio- und/oder Video- und/oder Animations- und/oder Simulations- und/oder Programmdatei ist.

12. Vorrichtung nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, dass die Dokumentdatenstruktur aus der Gruppe ausgewählt ist, die die Datenformate MP3, MPEG, XML aufweist.

13. Verfahren zum kopiergeschützten Verteilen elektronischer Dokumente einer vorbestimmten Dokumentdatenstruktur in einem öffentlich zugänglichen, elektroni-

schen Datennetz, insbesondere Verfahren zum Betreiben der Scripterzeugungseinheit nach einem der Ansprüche 6 bis 12, gekennzeichnet durch die Schritte:

- Empfangen einer Anfrage nach einem elektronischen Dokument von einer mit dem elektronischen Datennetz verbundenen Teilnehmereinheit;
- Abfragen von Datennetzadressen jeweiliger Speicherorte von einer Mehrzahl dem elektronischen Dokument zugehörigen Dateiabschnitten, die bei einer Mehrzahl von Teilnehmereinheiten verteilt gespeichert sind;
- Erstellen eines Ablaufbefehlssatzes, der die Datennetzadressen in einer vorbestimmten Reihenfolge enthält;
- Übertragen des Ablaufbefehlssatzes zu der Teilnehmereinheit, wobei der Ablaufbefehlssatz der Teilnehmereinheit das Zugreifen auf die Mehrzahl der Dateiabschnitte bei den betreffenden Teilnehmereinheiten und das teilnehmerseitige Abspeichern derselben in der vorbestimmten Reihenfolge ermöglicht.

14. Verfahren nach Anspruch 13, dadurch gekennzeichnet, dass die vorbestimmte Reihenfolge für die die Anfrage abgebenden Teilnehmereinheit individuell und identifizierend erstellt wird.

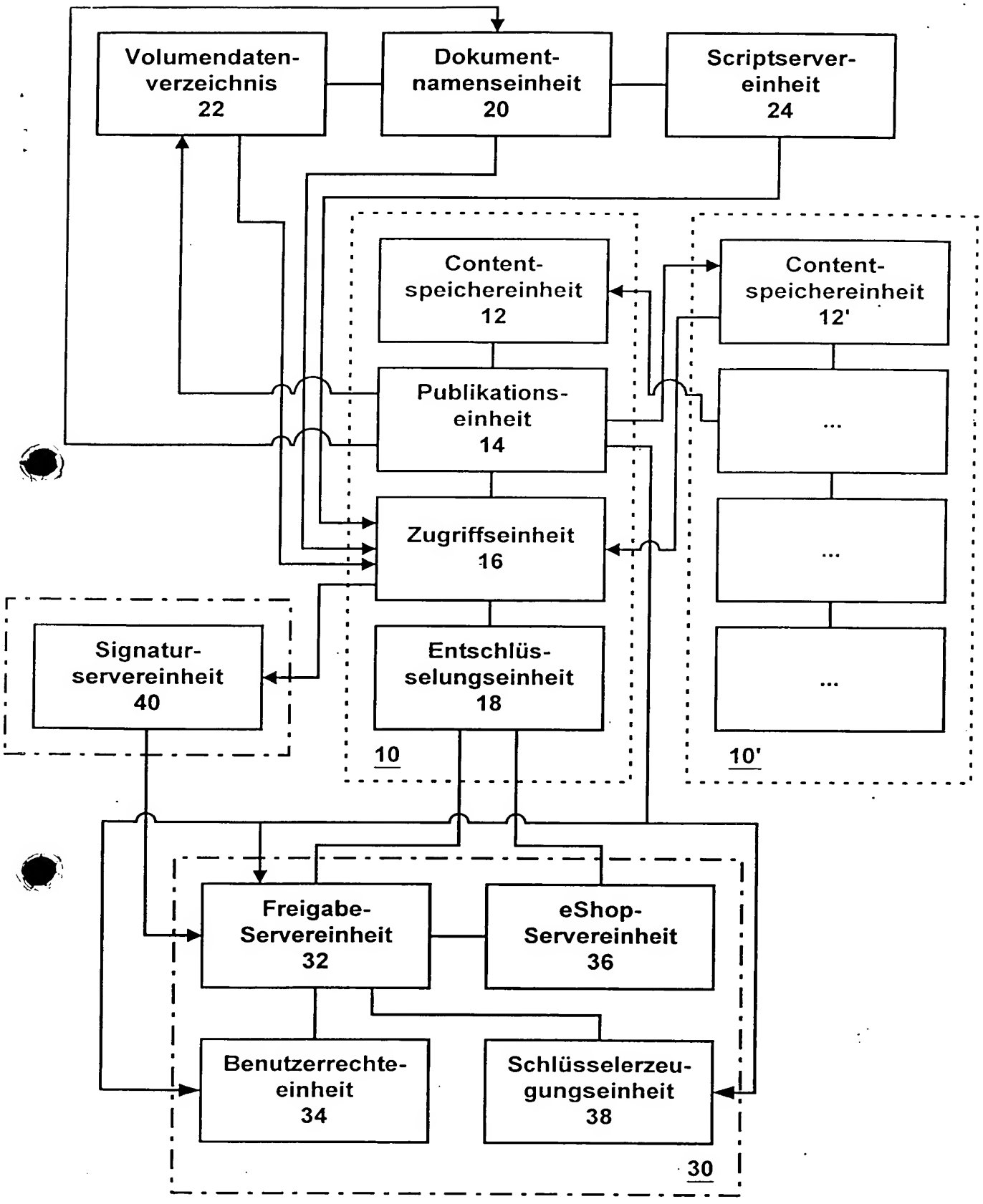
Volumendaten-
verzeichnis
22
Dokument-
namenseinheit
20
Scriptserver-
einheit
24
Content-
speichereinheit
12
Content-
speichereinheit
12'
Publikations-
einheit
14
...
Zugriffseinheit
16
...
Signatur-
servereinheit
40
Entschlüs-
selungseinheit
18
...
10
10'
Freigabe-
Servereinheit
32
eShop-
Servereinheit
36
Benutzerrechte-
einheit
34
Schlüsselerzeu-
gungseinheit
38
30

Fig. 1

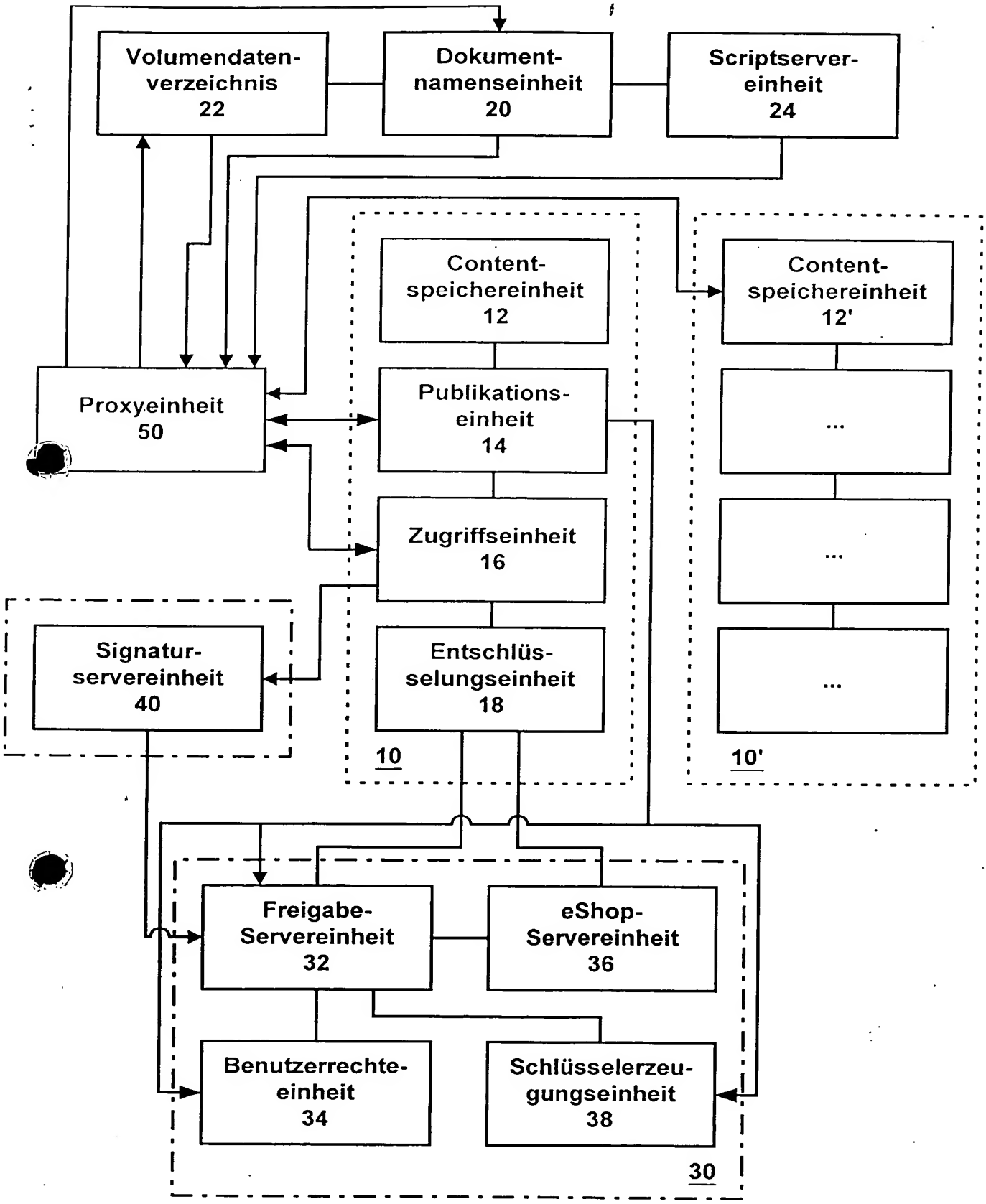
Volumendaten-
verzeichnis
22
Dokument-
namenseinheit
20
Scriptserver-
einheit
24
Content-
speichereinheit
12
Content-
speichereinheit
12'
Proxyeinheit
50
Publikations-
einheit
14
...
Zugriffseinheit
16
...
Signatur-
servereinheit
40
Entschlüs-
selungseinheit
18
...
10
10'
Freigabe-
Servereinheit
32
eShop-
Servereinheit
36
Benutzerrechte-
einheit
34
Schlüsselerzeu-
gungseinheit
38
30

Fig. 2